MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2022 / 2023 (TERM ID 2210)

BEL 1614 ELECTRONIC COMMERCE

(All Sections / Groups)

11 FEBRUARY 2023
09.00 A.M.- 12.00 P.M. (3 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages (including cover page) with 1 case study question
2. There are five sub sections for this case study question
3. Answer **ALL** questions
4. Mark distribution for each question is given in parenthesis

Case: Meltdown and Spectre Security Flaw affects Samsung Galaxy S7

Samsung Galaxy S7 users have been informed recently that there has been a serious security flaw in the microchip of the device. Hackers could potentially spy on users that could leave millions of users vulnerable to all sorts of Cyber-attacks. Samsung Electronics is the manufacturer of Galaxy S7 which experts thought had immunity to security vulnerability known as Meltdown and Spectre. This threat has affected most PCs, smartphones and other computing devices. In essence Meltdown and Spectre can affect both operating systems i.e. Android and iOS. A user's phone can be infected quite easily by just visiting a wrong website through a Javascript type malware.

Microprocessors undergo a process called "speculative execution" which is meant to make our smartphones and computers run faster. Tasks are predicted by the processor and the processor works in advanced on other tasks that a user might be interested to do and prepares for it. In other words, it works in parallels and does not conduct tasks sequentially to increase processing speed. As such certain check permissions are not done correctly and leak information about predictive tasks is not run eventually. These are dropped but theoretically glimpses of data in the kernel can be stolen due to this. Apple was quick to issue iOS security patches and this was also done by Samsung for their Android users. Likewise, Google also has issued security patches for Android, Pixel and Nexus users. According to experts virtually all machines that run on the Intel chip has been already infected by Meltdown and Spectre. Imagine that in the core of every computer system where millions of instructions are being processed (usually hardware chipset) and that core is now infected with a bug that can create chaos for users. Meltdown and Spectre could allow hackers to remotely steal passwords, emails, credit card information, e-wallet data and even your bank information.

Intel claims that the flaws in the processing core however will not allow unauthorized users to corrupt, modify or delete data. When experts discovered these vulnerabilities, they quickly disclosed the information to large technical companies like Apple, Intel and Microsoft based on known protocol that is "responsible disclosure". Now these companies are updating software patches for potential threats in terms of Confidentiality, Integrity, Authentication and Repudiation. Meanwhile Intel has been reticent about the specifics of vulnerabilities that might impact the user. A recent UNECE study revealed a 1300 percent increase of data growth since 2011 resulting thousands of ZB (ZetaByte) which now is being commonly associated with Big Data. By 2019, UNECE predicts that this growth will continue to reach 40,000 ZB of data. This will be more than what the world would have seen in the last 5,000 years combined.

Author:
Dr. Saravanan Muthaiyah, Professor, Faculty of Management, Research Institute for Digital Enterprise (RIDE), Multimedia University, 63100 Cyberjaya, Malaysia.

©2018 M Saravanan Muthaiyah, Multimedia University. All rights reserved.

Continued.....

Questions

a. Clarify e-commerce issues that are highlighted in this case? (12 marks)

b. Explain if "Speculative Execution" is good or bad? (12 marks)

c. Most users do not ever read the manual of any hardware or software but simply agree to the terms and exclusion clauses of online contracts. Do you think they have brought this upon themselves, and they should solely be blamed? Describe why or why not?

(20 marks)

d. Will the security patches do the trick? Describe why or why not? (9 marks)

e. With the exponential growth of data and volumes of online transactions, clarify if you think transacting on the Blockchain will solve all vulnerability issues?

(7 marks)

End of Paper